Лекция 2

Теорема 1. *Отношение изоморфности – это отношение эквивалентности.*

Доказательство. Нужно проверить, что отношение изоморфности удовлетворяет свойствам рефлексивности, симметричности и транзитивности. В самом деле. Тождественное преобразование задает изоморфизм любой группы с собой. Рефлексивность доказана. Если $\varphi\colon G \to H$ – изоморфизм, то в частности это биекция. Тогда существует обратное отображение φ^{-1}. Оно также является гомоморфизмом. В самом деле, пусть $a, b \in H$, в силу сюръективности φ, имеем $a = \varphi(u)$, $b = \varphi(v)$ для некоторых $u, v \in G$. Тогда $\varphi^{-1}(ab) = \varphi^{-1}(\varphi(u)\varphi(v)) = \varphi^{-1}(\varphi(uv)) = uv = \varphi^{-1}(a)\varphi^{-1}(b)$. Таким образом, φ^{-1} – изоморфизм. Симметричность доказана. Докажем, что композиция двух изоморфизмов – изоморфизм. Пусть $\varphi\colon G \to H$ и $\psi\colon H \to F$ – два гомоморфизма. Тогда

$$\psi \circ \varphi(g_1g_2) = \psi(\varphi(g_1g_2)) = \psi(\varphi(g_1)\varphi(g_2)) = \psi(\varphi(g_1))\psi(\varphi(g_2)) = \psi \circ \varphi(g_1)\psi \circ \varphi(g_2).$$

То есть $\psi \circ \varphi$ – гомоморфизм. С другой стороны, $\psi \circ \varphi$ – биекция. Значит, $\psi \circ \varphi$ – изоморфизм. Транзитивность доказана. □

Из этого предложения следует, что все группы распадаются на непересекающиеся классы изоморфности.

Приведем еще один пример группы.

Пример 1. *Группа комплексных корней из единицы n-ой степени. Пусть μ_n – множество всех комплексных корней степени n из 1. Тогда $(\mu_n, \cdot)$ – абелева группа порядка n. Докажем это. Для того, чтобы доказать, что μ_n – группа мы воспользуемся, тем, что это подмножество в известной нам группе $\mathbb{C}^\times$. Нам надо лишь проверить, что μ_n замкнуто относительно умножения и взятия обратного. Пусть $a, b \in \mu_n$, то есть $a^n = b^n = 1$. Тогда $(ab)^n = a^n b^n = 1$, значит, $ab \in \mu_n$. Мы доказали, что μ_n замкнуто относительно умножения. С другой стороны $(a^{-1})^n = (a^n)^{-1} = 1^{-1} = 1$, следовательно, μ_n замкнуто относительно взятия обратного. То, что группа μ_n абелева следует из того, что она является подгруппой в абелевой группе $\mathbb{C}^\times$.*

Установим следующий изоморфизм групп.

Пример 2. *Группа $\mathbb{Z}_n$ изоморфна группе μ_n. Один из возможных автоморфизмов переводит $k \in \mathbb{Z}_n$ в $\cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}$. То, что φ – гомоморфизм обеспечивается тем, что при умножении комплексных чисел их аргументы складываются.*

Определим группу, которая называется *группой кватернионов.*

Пример 3. *Группа кватернионов Q_8. Рассмотрим множество из 8 элементов:*

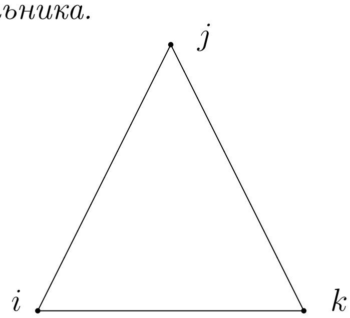
$$\{1, -1, i, -i, j, -j, k, -k\}.$$

Умножение устроено следующим образом: знаки умножаются отдельно,

$$i^2 = j^2 = k^2 = -1,$$

$$ij = k,\ ji = -k,\ ik = -j,\ ki = j,\ jk = i,\ kj = -i.$$

Для того, чтобы запомнить правило умножения элементов i, j и k удобно изобразить их в вершинах треугольника.



Теперь, если мы хотим умножить два элемента, то, если направление движение от первого ко второму по часовой стрелке, получаем третий элемент, а если против часовой стрелки, то минус третий.

Легко видеть, что 1 – нейтральный элемент, и каждый элемент обратим. В самом деле, элементы 1 *и* -1 *являются обратными к самим себе. А для любого другого элемента x выполнено $x^{-1} = -x$. Для того, чтобы утверждать, что Q_8 – группа, необходимо проверить ассоциативность. Перейдем к доказательству этого.*

Напомним, что изоморфизм (биективное соответствие, переводящее умножение одной группы в умножение другой) можно задать в случае, когда про одну из структур не известно, группа это или нет. Тогда вторая структура будет автоматически группой. На прошлой лекции мы доказали следующую теорему

Теорема 2. *Пусть G – группа, а H – группоид. И пусть $\varphi\colon G \to H$ – биекция и гомоморфизм (то есть $\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2)$. (Можно сказать, что φ – изоморфизм группоидов.) Тогда H – также группа и φ – изоморфизм групп.*

Теперь мы готовы доказать, что Q_8 – группа.

Предложение 1. Q_8 *– группа*

Доказательство. Рассмотрим следующее множество из 8 комплексных матриц, которое мы обозначим $\overline{Q}_8$.

$$\left\{\pm\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},\ \pm\begin{pmatrix}\mathrm{i} & 0\\ 0 & -\mathrm{i}\end{pmatrix},\ \pm\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix},\ \pm\begin{pmatrix}0 & \mathrm{i}\\ \mathrm{i} & 0\end{pmatrix}\right\}.$$

Здесь i – это мнимая единица (комплексное число).

Рассмотрим биекцию φ между Q_8 и $\overline{Q}_8$.

$$\pm1 \mapsto \pm\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},\ i \mapsto \pm\begin{pmatrix}\mathrm{i} & 0\\ 0 & -\mathrm{i}\end{pmatrix},\ j \mapsto \pm\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix},\ k \mapsto \pm\begin{pmatrix}0 & \mathrm{i}\\ \mathrm{i} & 0\end{pmatrix}.$$

Легко убедиться, что φ переводит умножение в Q_8 в матричное умножение. Следовательно, $(\overline{Q}_8, \cdot)$ – это замкнутое относительно умножения и взятия обратной матрицы подмножество в $\mathrm{GL}_2(\mathbb{C})$. Значит, $\overline{Q}_8$ – подгруппа. Тогда, по теореме 2, Q_8 – группа, изоморфная $\overline{Q}_8$. $\square$

Определение 1. Пусть g – элемент группы G, а n – целое число. Определим n-ю степень элемента g следующим образом. Если n положительное, то $g^n = g \cdot \ldots \cdot g$ – произведение n элементов g. Если n отрицательное, то $g^n = (g^{-1})^n$. Нулевая степень любого элемента равна нейтральному элементу e.

Упражнение 1. Выполнены следующие свойства степеней элемента группы:
1) $g^m g^n = g^{m+n}$,
2) $(g^m)^n = g^{mn}$

Указание. Рассмотреть все случаи знаков m и n.

Определение 2. Пусть g – элемент группы G. Порядок g – это минимальное натуральное число n такое, что $g^n = e$. Если такого числа не существует, то порядок элемента g равен бесконечности. Порядок элемента g обозначается $\operatorname{ord}(g)$.

Определение 3. Группа G называется *циклической*, если найдется элемент $g \in G$ такой, что каждый элемент G имеет вид g^k для некоторого целого числа k.

Элемент g называется *порождающим элементом группы* G, при этом группа G обозначается $\langle g \rangle$.

Замечание 1. В предыдущем определении не требуется, чтобы все степени g были различны.

Пример 4. *а) Группа* $\mathbb{Z}$ *является циклической. В самом деле,* $\mathbb{Z} = \langle 1 \rangle$.
б) Аналогично $\mathbb{Z}_n = \langle 1 \rangle$.

Лемма 1. *Циклическая группа* $\langle g \rangle$ *изоморфна*
- $\mathbb{Z}_n$ *при условии* $\operatorname{ord} g = n$*;*
- $\mathbb{Z}$ *при условии* $\operatorname{ord} g = \infty$.

Доказательство. Пусть $\operatorname{ord} g = n$. Рассмотрим множество элементов

$$S = \{g^0 = e, g, g^2, \dots g^{n-1}\}.$$

Докажем, что все элементы группы $\langle g \rangle$ лежат в S и что все элементы S различны. В самом деле, пусть g^k – некоторый элемент $\langle g \rangle$. Разделим k на n с остатком: $k = nm + r$, где $0 \le k < n$. Тогда $g^k = (g^n)^m g^r = g^r \in S$.

С другой стороны. Пусть $0 \le a < b < n$ и $g^a = g^b$. Умножая последнее равенство на g^{-a}, получаем $e = g^{b-a}$. Поскольку $0 < b - a < n$, это противоречит тому, что $\operatorname{ord}(g) = n$.

Рассмотрим отображение $\psi\colon \mathbb{Z}_n \to \langle g \rangle$, $\psi(k) = g^k$. Элементы $\mathbb{Z}_n$ – это не числа, а классы чисел с одинаковым остатком. Поэтому нам надо доказать, что отображение ψ определено корректно. А именно, пусть $k' = mn + k$ для некоторого $m \in \mathbb{Z}$. Тогда $\psi(k') = g^{k'} = (g^n)^m g^k = g^k = \psi(k)$. Корректность доказана. Теперь проверим, что ψ – гомоморфизм. Действительно, $\psi(k + l) = g^{k+l} = g^k g^l = \psi(k)\psi(l)$. Заметим, что $\mathbb{Z}_n$ состоит из классов чисел $0, 1, \dots, n-1$. При отображении ψ эти классы переходят в элементы множества S. Причем это отображение очевидно сюръективно и инъективно так как элементы S не совпадают. Итак, ψ – гомоморфизм и биекция, то есть изоморфизм.

Пусть теперь $\operatorname{ord} g = \infty$. Рассмотрим отображение $\psi\colon \mathbb{Z} \to \langle g \rangle$, $\psi(k) = g^k$. Как и в прошлом случае получим, что ψ – гомоморфизм. (В этом случае проверять корректность не нужно, так как элементы $\mathbb{Z}$ – числа, а не классы чисел.) Сюръективность ψ следует из определения циклической группы. Докажем инъективность. Предположим, что $g^a = g^b$, где $a > b$. Домножим это равенство на g^{-b} и получим $g^{a-b} = e$, что противоречит тому, что $\operatorname{ord} g = \infty$. Итак, ψ – гомоморфизм и биекция, то есть изоморфизм. $\square$

Если известно, что порядок g равен n, то группу $\langle g \rangle$ обозначают $\langle g \rangle_n$.

Замечание 2. Для каждого элемента g некоторой группы G можно рассмотреть циклическую подгруппу, порожденную этим элементом: $\langle g\rangle \subset G$.

Лемма 2. *Пусть g – элемент группы G такой, что* $\mathrm{ord} g = n$, *а m – целое число. Тогда*
$$\mathrm{ord} g^m = \frac{n}{\textit{НОД}(m,n)} = \frac{\textit{НОК}(m,n)}{m}.$$

Доказательство. Докажем это утверждение только для положительных m, так как $\mathrm{ord}(g^{-m}) = \mathrm{ord}((g^m)^{-1}) = \mathrm{ord}(g^m)$, а также $\mathrm{ord}(g^0) = 1$.

Рассмотрим группу $\langle g\rangle$. По предыдущей лемме она изоморфна $\mathbb{Z}_n$. Более того при построенном изоморфизме этих групп элемент g соответствует $1 \in \mathbb{Z}_n$, и элемент g^m соответствует $m \in \mathbb{Z}_n$. Таким образом, нам нужно доказать, что порядок $m \in \mathbb{Z}_n$ равен $\frac{n}{\text{НОД}(m,n)} = \frac{\text{НОК}(m,n)}{m}$. Порядок – это такая минимальная натуральная степень k, в которой элемент равен e. В аддитивных обозначениях получаем $\mathrm{ord}(m) = k$, если k – это минимальное натуральное число такое, что $mk = 0$ в $\mathbb{Z}_n$. Для целых чисел условие перепишется как mk делится на n. Получается, что mk – общее кратное m и n. Таким образом, $k \geq \frac{\text{НОК}(m,n)}{m}$.С другой стороны $k = \frac{\text{НОК}(m,n)}{m}$ подходит, так как $mk = \frac{\text{НОК}(m,n)}{m}m = \text{НОК}(m,n)$ делится на n. $\square$

Теорема 3. *1) Подгруппа циклической группы циклическая;*

2) Все подгруппы $\mathbb{Z}$ имеют вид $\langle k\rangle = k\mathbb{Z} \cong \mathbb{Z}$;

3) Все подгруппы $\mathbb{Z}_n$ имеют вид $\langle d\rangle = d\mathbb{Z}_n \cong \mathbb{Z}_{\frac{n}{d}}$ для некоторого d – делителя n;

4) Пусть $m \in \mathbb{Z}_n$. Тогда $\langle m\rangle = \langle \textit{НОД}(m,n)\rangle$.

Доказательство. 1) Следует из пунктов 2) и 3).

2) Пусть H – подгруппа в $\mathbb{Z}$. Если $H = \{0\}$, то $H = \langle 0\rangle$, что укладывается в утверждение задачи. Пусть $H \neq \{0\}$. Если $h \in H$ – отрицательное число, то положительное число $-h$ также лежит в H. Значит, в H есть натуральные числа. Выберем k – минимальное натуральное число из H. Пусть $h \in H$. Тогда $h = kq + r$, где $0 \leq r < k$. При этом $kq \in H$, $h \in H$, следовательно, $r \in H$. Если $r \neq 0$, получаем противоречие с выбором k. Значит, $r = 0$ и h делится на k. Отсюда $H = \langle k\rangle$.

3) Пусть H – подгруппа в $\mathbb{Z}_n$. Если $H = \{0\}$, то $H = \langle n\rangle$, что укладывается в утверждение задачи. Пусть $H \neq \{0\}$. Рассмотрим минимальное натуральное число d такое, что его класс лежит в H. Ясно, что $d < n$. Пусть $h \in H$. Тогда $h = dq + r$, где $0 \leq r < d$. При этом $dq \in H$, $h \in H$, следовательно, $r \in H$. Если $r \neq 0$, получаем противоречие с выбором d. Значит, $r = 0$ и h делится на d. Отсюда $H = \langle d\rangle$. Докажем, что d – делитель n. Если это не так, то $n = kd + s$, $0 < s < d$. Но тогда в $\mathbb{Z}_n$ выполнено $s = kd \in H$, противоречие с выбором d. Итак, d – делитель n. Осталось сказать, что порядок d в группе $\mathbb{Z}_n$ равен $\frac{n}{d}$. Значит, $H = \langle d\rangle \cong \mathbb{Z}_{\frac{n}{d}}$.

4) $\langle m\rangle$ – циклическая группа. По лемме 2, $\mathrm{ord}(m) = \frac{n}{\text{НОД}(m,n)}$. Значит $|\langle m\rangle| = \frac{n}{\text{НОД}(m,n)}$. Следовательно, по пункту 3), $\langle m\rangle = \langle \text{НОД}(m,n)\rangle$. $\square$

Определение 4. Пусть H – подгруппа группы G. Рассмотрим элемент $g \in G$. *Левым смежным классом элемента g по подгруппе H* называется множество
$$gH = \{gh \mid h \in H\}.$$

Правым смежным классом элемента g по подгруппе H называется множество
$$Hg = \{hg \mid h \in H\}.$$

Лемма 3. *1) $g \in fH$ тогда и только тогда, когда $f^{-1}g \in H$,*

1') $g \in Hf$ тогда и только тогда, когда $gf^{-1} \in H$,

2) Левые (правые) смежные классы – это классы эквивалентности. (Более точно, отношение $g \sim f$, если $g \in fH$ является отношением эквивалентности.)

3) Следующие мощности одинаковы $|gH| = |Hg| = |H|$.

Доказательство. 1) $g \in fH \iff g = fh \iff f^{-1}g = h$.

1') $g \in Hf \iff g = hf \iff gf^{-1} = h$.

2) Докажем только для левых смежных классов. Для правых аналогично.

Рефлексивность: $g \in gH$ так как $e \in H$,

Симметричность:

$$g \in fH \iff f^{-1}g \in H \iff (f^{-1}g)^{-1} = g^{-1}f \in H \iff f \in gH.$$

Транзитивность:

$$g \in fH, f \in sH \Longrightarrow f^{-1}g \in H, s^{-1}f \in H \Longrightarrow s^{-1}ff^{-1}g = s^{-1}g \in H.$$

3) Следует из того, что $gh_1 = gh_2$ тогда и только тогда, когда $h_1 = h_2$. □

Замечание 3. Из пункта 2 следует, что левые (правые) смежные классы либо не пересекаются, либо совпадают.

Определение 5. Индекс подгруппы H группы G – это мощность множества левых смежных классов. Обозначается индекс $[G : H]$

Задача 1. Докажите, что $gH \leftrightarrow Hg^{-1}$ – биекция между левыми и правыми смежными классами, и следовательно мощность правых смежных классов также равна индексу подгруппы. (То, что количество левых и правых смежных классов одинаково для конечной группы будет следовать из теоремы Лагранжа, но это верно и для бесконечных групп.)

Теорема 4. *(Лагранж) Пусть G – конечная группа и H – подгруппа G. Тогда*

$$|G| = |H| \cdot [G : H].$$

Доказательство. Поскольку каждый элемент группы G лежит в некотором левом смежном классе и левые смежные классы либо совпадают, либо не пересекаются, вся группа G разбивается на непересекающиеся левые смежные классы. Так как мощность каждого смежного класса равна $|H|$, мощность всей группы равна $|H|$ умножить на количество смежных классов. □

Следствие 1. *(Следствия из теоремы Лагранжа)*

1) Порядок конечной группы делится на порядок ее подгруппы.

2) Порядок конечной группы делится на порядок ее элемента.

3) Для любого элемента g конечной группы G выполнено $g^{|G|} = e$.

4) Группа простого порядка циклическая.

5) (Малая теорема Ферма) Пусть p – простое число и a – число, не делящееся на p. Тогда a^{p-1} имеет остаток 1 при делении на p.

Доказательство. 1) Очевидно следует из теоремы Лагранжа.

2) Пусть g – элемент конечной группы G. Рассмотрим циклическую подгруппу $H = \langle g \rangle$. Поскольку $\mathrm{ord}(g) = |H|$, порядок G делится на $\mathrm{ord}(g)$.

3) Пусть $|G| = \mathrm{ord}(g) \cdot k$. Тогда $g^{|G|} = (g^{\mathrm{ord}(g)})^k = e^k = e$.

4) Пусть $|G| = p$ – простое число. Рассмотрим $g \neq e \in G$. Поскольку порядок g делит p и не равен 1, получаем $\mathrm{ord}(g) = p$. А значит, $G = \langle g \rangle$.

5) Применим пункт 3 к группе $\mathbb{Z}_p^\times = (\mathbb{Z}_p \setminus \{0\}, \cdot)$ и ее элементу a. Получаем

$$a^{|\mathbb{Z}_p^\times|} = a^{p-1} = 1(\mathrm{mod}\ p).$$

$\square$